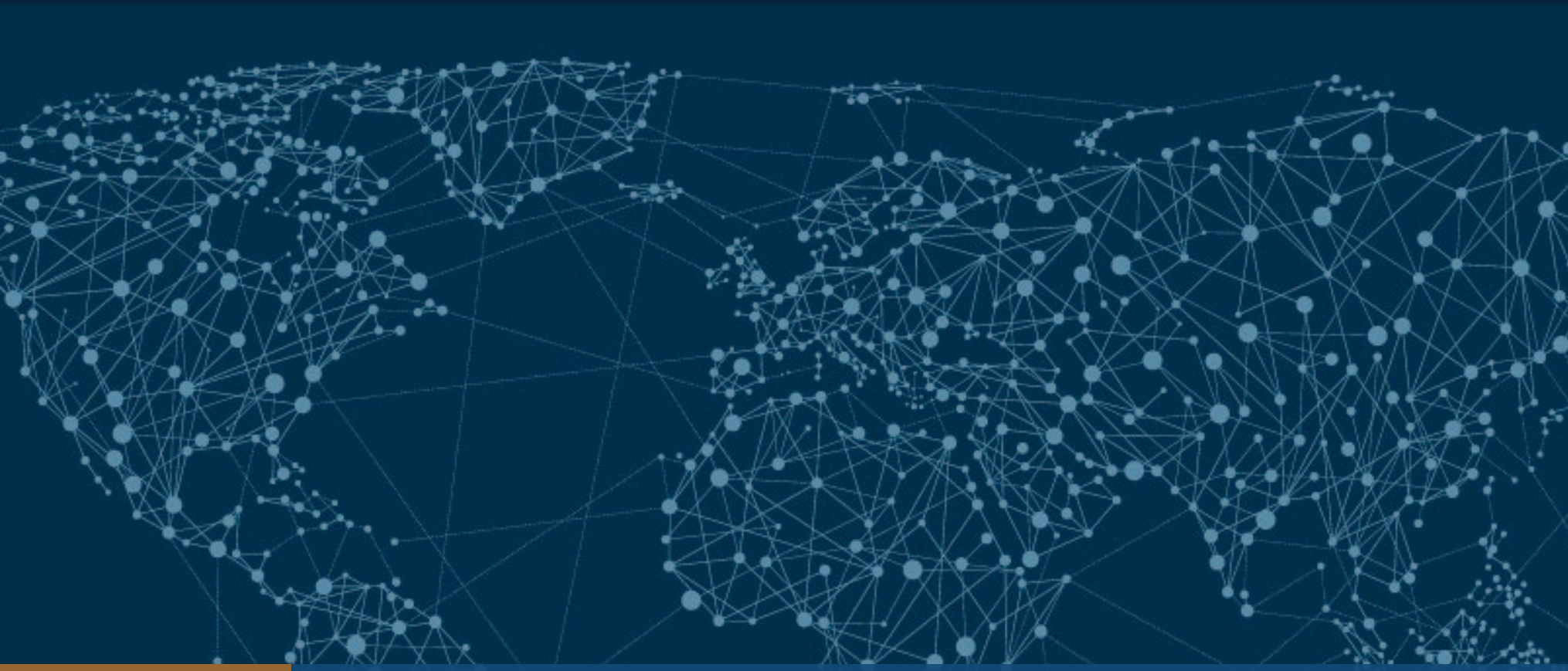


Update on Whois-related initiatives

GAC PSWG | ICANN 57 | 5 November 2016

Goals and Expected Outcomes of this Session

1. Update on **Whois initiatives**
2. **Accountability** as a lens
3. **Sharing views** for consideration and identifying common elements

Session Chaired by:
Alice Munyua - African Union Commission GAC Representative, PSWG co-Chair

Discussion Moderated by:
Cathrin Bauer-Bulst - European Commission, GAC PSWG

Agenda & Speakers

1) Introduction — Cathrin Bauer-Bulst (EU Commission)

2) Public Safety Use of Whois — Gregory Mounier (Europol)

3) Whois Today

- Whois Accuracy Reporting System (ARS)
  Jared Erwin (ICANN GDD)
- Contractual Compliance
  Maguy Serad
  (ICANN Contractual Compliance)
- Thick Whois, RDAP, Translation & Transliteration
  Krista Papac (ICANN GDD)

4) The future of Whois/RDS

- RDS Review Team
  Margie Milam (ICANN MSSI)
- Registration Directory Services Policy Development Process (PDP)
  Chuck Gomes (Chair, RDS PDP WG)
- Privacy & Proxy Services Accreditation
  Graeme Bunton (co-Chair PPSAI PDP WG)

EUROPOL
EC3 | European Cybercrime Centre

PUBLIC SAFETY USE OF THE WHOIS

ICANN 57 - Hyderabad

HIT WHOIS

4 November 2016

Gregory Mounier
Head of Outreach
European Cybercrime Centre (EC3)
EUROPOL

Uses of the WHOIS

Traditionally:

- Contact point for incident response
- Determination of availability of domain names

But also:

- Assisting, public safety organisations, businesses, consumer groups, individuals in combating abuse and fraud and seeking redress.
- Help with online crime attribution

Public Safety Use of WHOIS

- WHOIS is one cyber investigative tool among many others
- WHOIS is not a silver bullet
- Accurate WHOIS => life of criminals more difficult
- Prevent exploitation of domain registration procedures

Botnet and DNS abuse

- DNS abuse at the heart of C&C infrastructure
- Getting new domain names from registrars around the world at fast pace:

✓ Sustain takedown requests

✓ Sustain sink holing attempts

✓ Sustain hijacking attempts

Botnets - Positive example

- **FP Cyborg** identified a suspect with WHOIS data
- WHOIS lookup on the domain => email address
- Reverse WHOIS lookup => other domains registered with same email
- Domain => Old private website
- Successful arrest and conviction

Child sexual exploitation

http://stella.artmodelingstudios.com

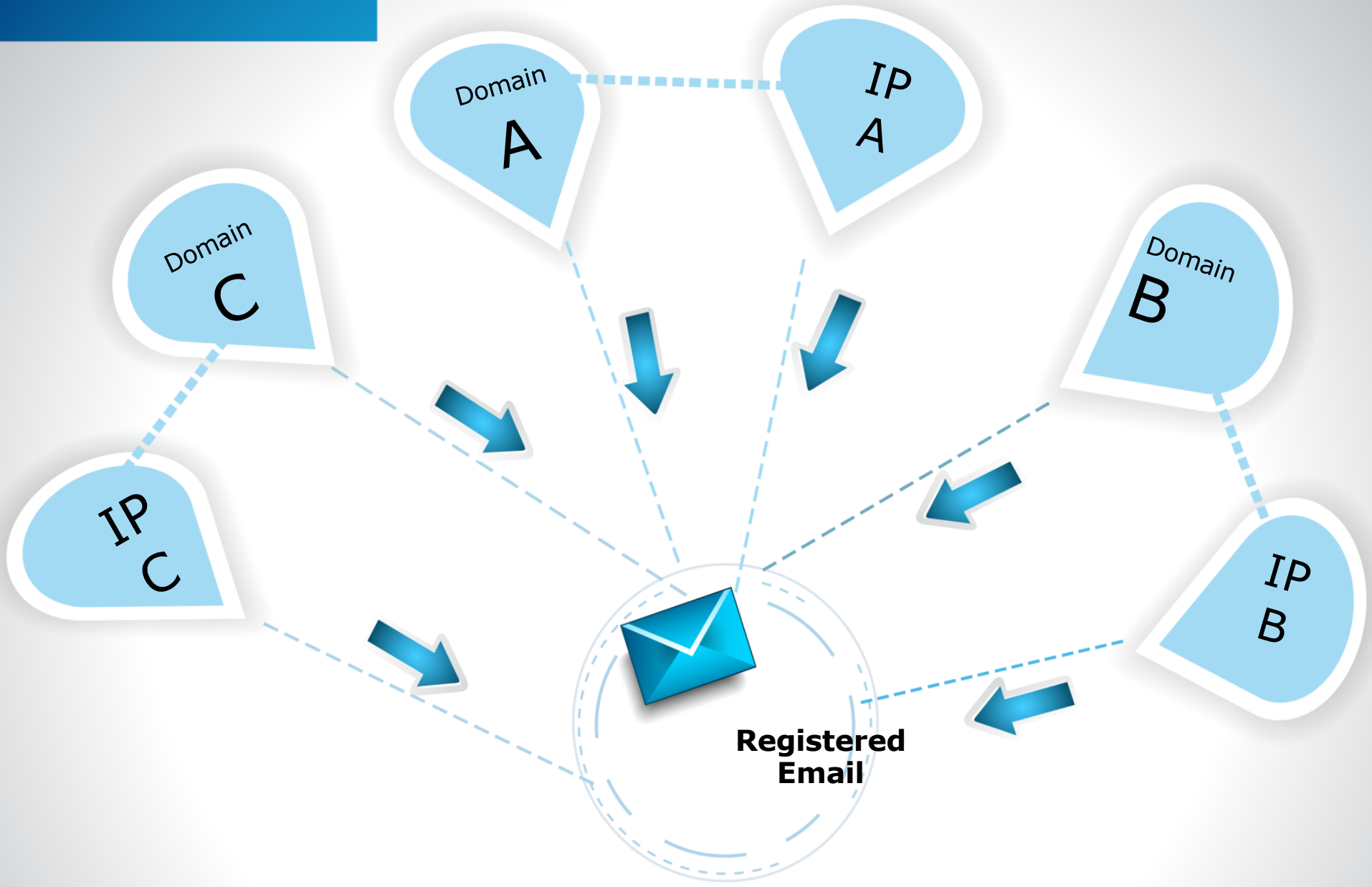
Reg: LV
Host:HU

http://forever.artmodelingstudios.com/

Reg: LV
Host:NL (ecatel)

Child sexual exploitation

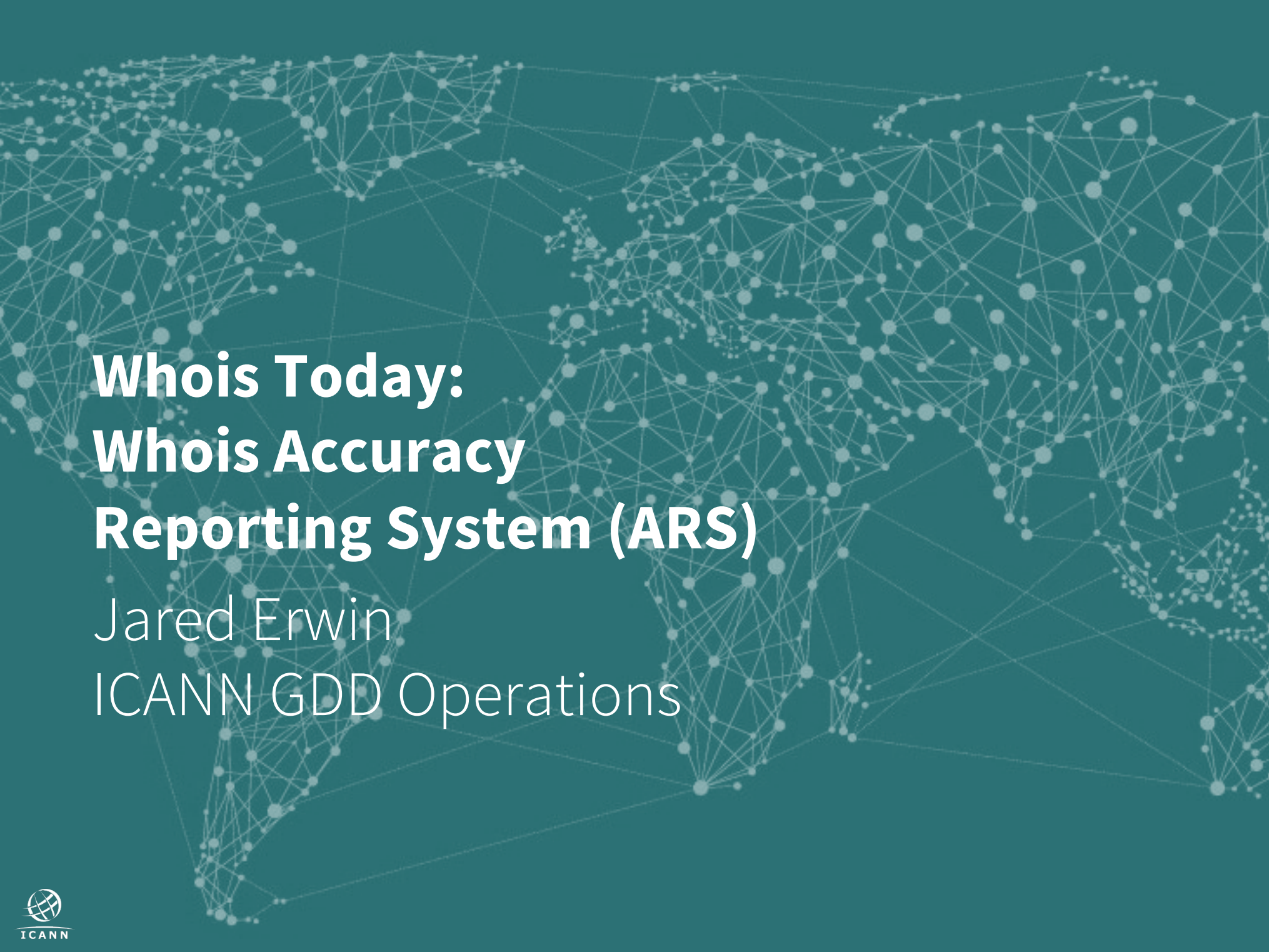
- Gather Domain names linked to those websites
- Gather DNS information linked to domain names.
- Gather WHOIS data linked to those domains
- Cross-match 3 data sets => identify valid email address


Domain
A
IP
A
Domain
C
Domain
B
IP
C
IP
B
Registered
Email

Conclusion

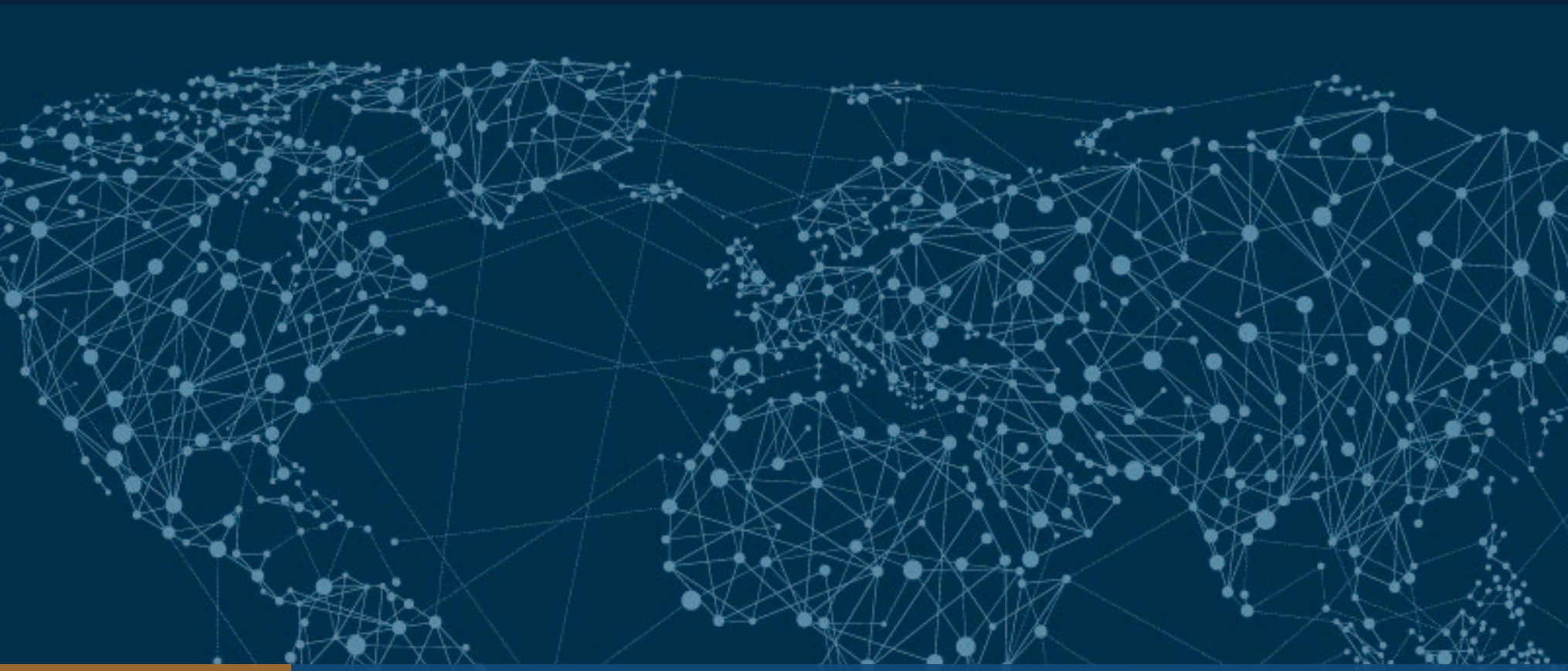
Accurate and reliable WHOIS data +
Publicly available:

- ✓ Helps crime attribution
- ✓ Saves precious investigation time (victims)
- ✓ Makes life of criminals more difficult
- ✓ Prevents abuse of domain registration procedures



Whois Today: Whois Accuracy Reporting System (ARS)

Jared Erwin
ICANN GDD Operations



WHOIS Accuracy Reporting System (ARS): Purpose and Outcomes

ICANN GDD Operations
5 November 2016

WHOIS ARS Background

- The ARS was designed to meet several recommendations from the 2012 WHOIS Review Team as well as address GAC advice on WHOIS accuracy (https://www.icann.org/resources/files/final-report-2012-05-11-en)

- The ARS has been implemented in phases based on the types of accuracy validation identified in SAC058 (https://www.icann.org/en/system/files/files/sac-058-en.pdf)

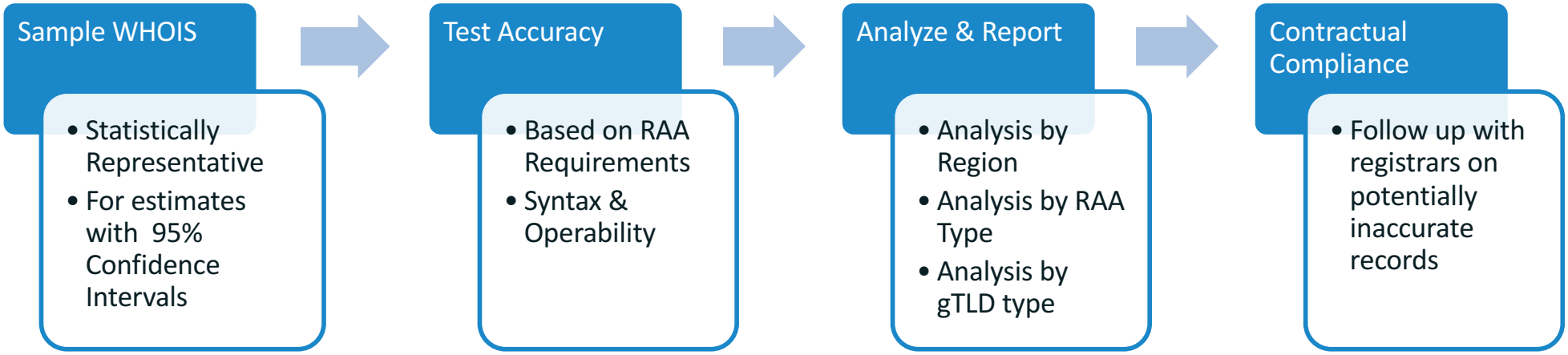
  - **Pilot Phase** - "Proof of Concept": Tested processes for data collection and validation
    - Report: Published 23 December 2014
    - Public Comment Report: Published 3 April 2015

  - **Phase 1** – Syntax Accuracy only; Is the record correctly formatted?
    - Report: Published 24 August 2015

  - **Phase 2** – Syntax + Operability Accuracy; Does the email go through, phone ring, mail deliver?
    - Cycle 1 Report: Published 23 December 2015
    - Cycle 2 Report: Published 8 June 2016
    - Cycle 3 Report: Expected December 2016
    - Cycle 4 Report: Expected June 2017

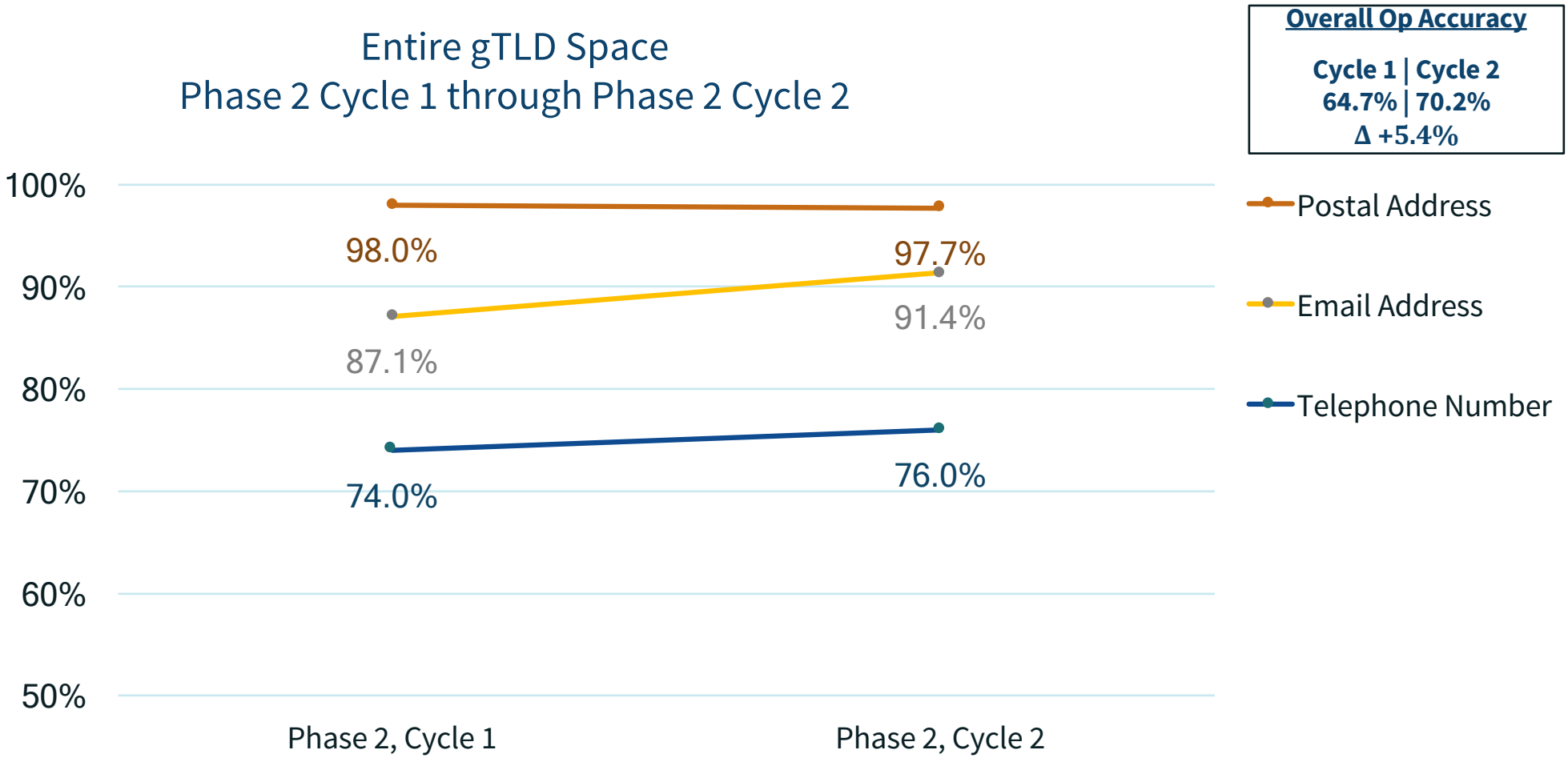
  - Reports can be found online at: https://whois.icann.org/en/whoisars-reporting

WHOIS ARS Process



- Each Cycle from Sample to Report takes approximately 6 Months
- The reports provide accuracy estimates within 95% confidence intervals
- ICANN performs these assessments twice per year

Sample Results - Phase 2 Cycle 2 – Changes Over Time: Operability Accuracy by Contact Mode



- Saw mostly improvement from Cycle 1 to Cycle 2
  - Changes in accuracy are mostly due to natural sample variation
- We eventually expect to see changes due to outreach by ICANN Contractual Compliance

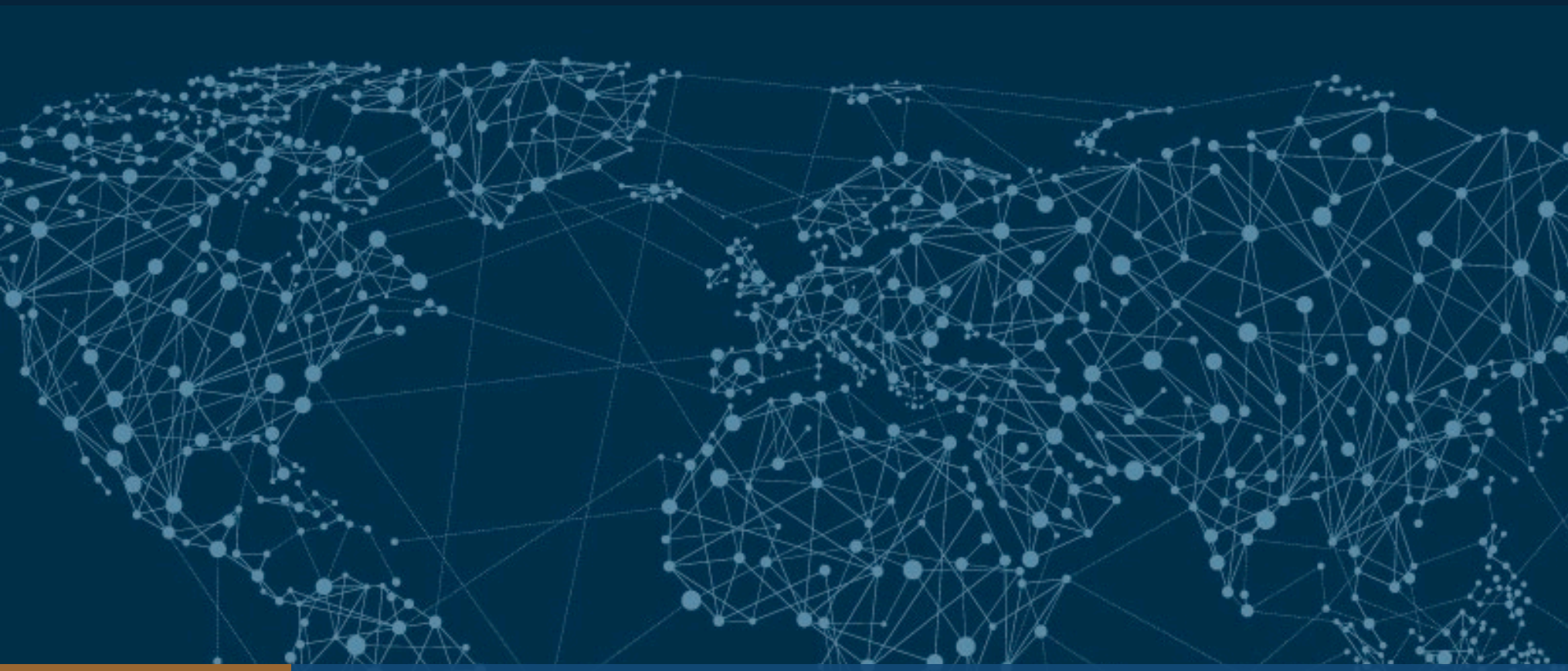
From WHOIS ARS to ICANN Contractual Compliance

- Potentially inaccurate records are provided to ICANN Contractual Compliance
- As the Cycles progress we expect to see overall improvements in accuracy
- In June 2016, the Contractual Compliance team began processing WHOIS Accuracy Reporting System (ARS) Phase 2, Cycle 2 complaints
- **Next step:** Phase 2 Cycle 3 results were provided to ICANN Contractual Compliance in mid-October to begin processing

Whois Today: Contractual Compliance

Maguy Serad
VP, Contractual Compliance Services

ICANN



Contractual Compliance Whois Compliance Efforts

WHOIS Related Compliance Efforts

Proactive Approach

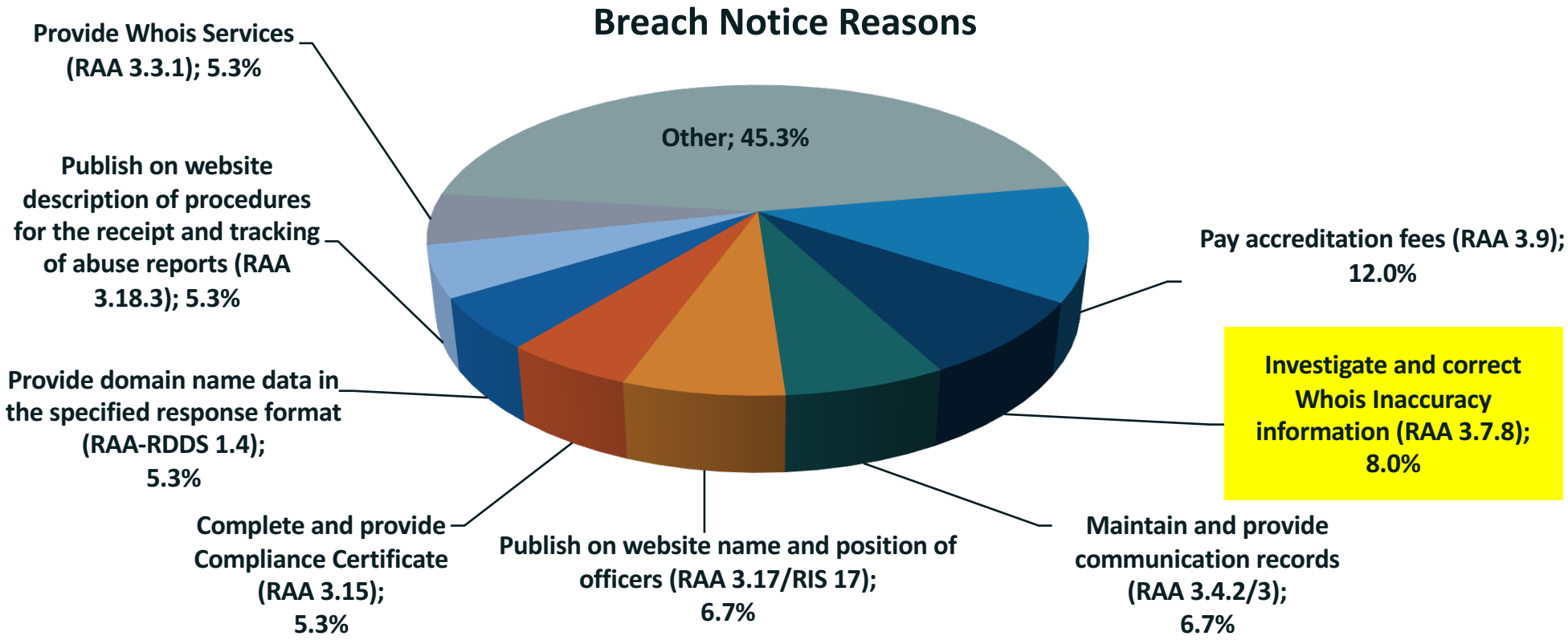
- Improved reporting and breakdown of WHOIS Inaccuracy monthly dashboard
- On-going outreach activities with contracted parties
  - On site outreach sessions in Seoul, Korea and China with contracted parties, https://www.icann.org/resources/compliance/outreach
  - Outreach via conference calls
- Monitoring and reviews based on systemic issues identified via complaints received or community concerns
- Remediation reviews to test and validate past remediation efforts
- On-going Audit activities that include WHOIS related reviews


Additional metrics on WHOIS

Global Formal Notice Activity (Feb 2016 – Sep 2016)

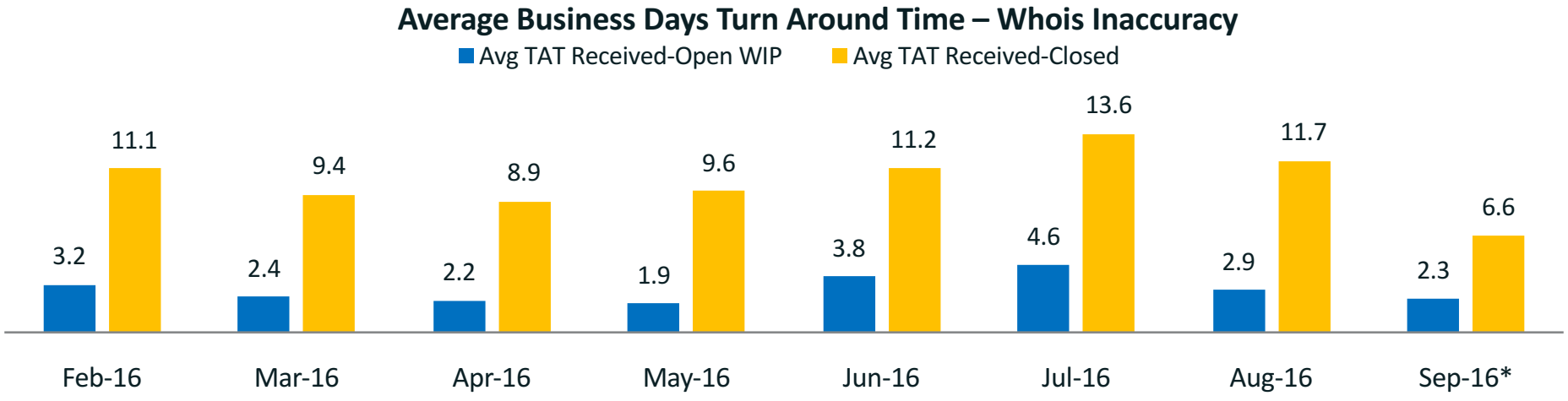
Notices	Qty
Breach	16
Non-Renewal	0
Suspension	2
Termination	2

Breach Notice Reason	Qty
Breach Notice Reasons	76
• Cured	57
• Not Cured	19

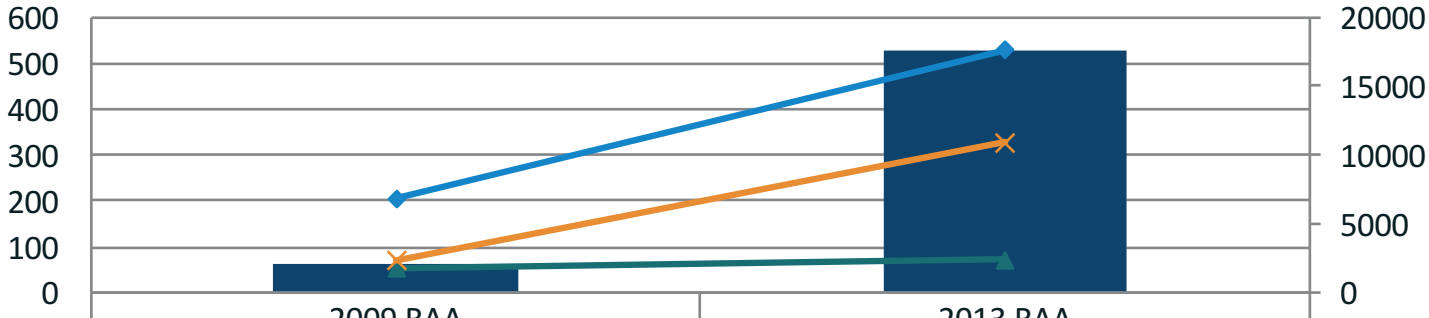


Disclaimer: Due to rounding, percentages may not always appear to add up to 100%.

WHOIS Related Metrics



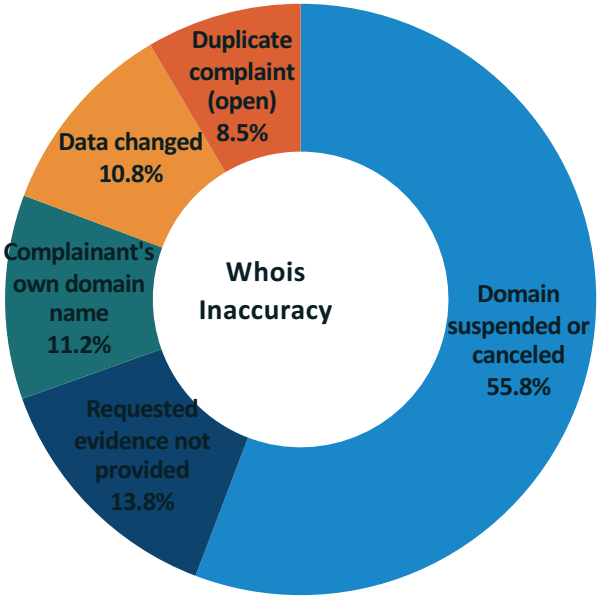
Registrar Complaints by Contract Year
Feb 2016 – Sep 2016

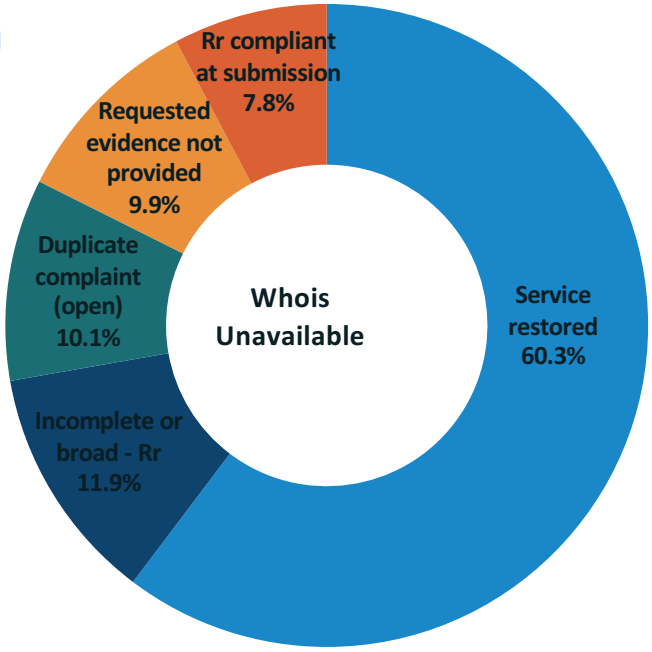


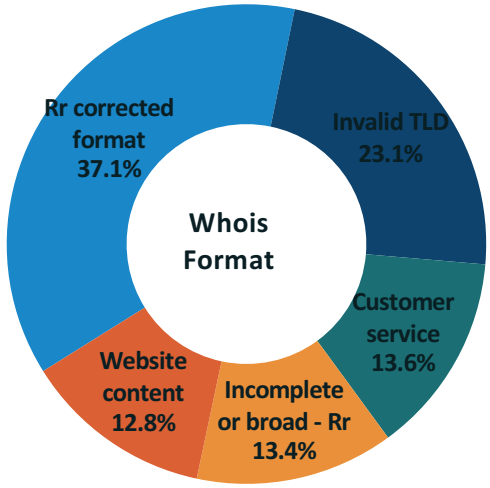
	2009 RAA	2013 RAA
WHOIS INACCURACY*	2,147	17,539
WHOIS FORMAT	206	529
WHOIS SLA	53	73
WHOIS UNAVAILABLE	70	329

** Includes Whois Inaccuracy, Whois QR & Whois ARS*

WHOIS Top Closure Reasons (Feb 2016 – Sep 2016)







Disclaimer: Due to rounding, percentages may not always appear to add up to 100%.

Whois Today: Thick Whois, RDAP, Translation & Transliteration

Krista Papac
Director, Registry Services, ICANN

ICANN

Thick Whois Policy Recommendations – Background

ICANN board adopted GNSO policy recommendations requiring all gTLD registries to **provide thick Whois services** with a **consistent labeling and display** (February 2014).

GNSO PDP Working Group concluded requiring Thick Whois:

- Would improve stability of and access to Whois data
- May reduce acquisition and processing costs for consumers of Whois data
- Would provide a more level playing field between registry providers

Thick Whois Policy Recommendations – Current Status

The implementation team divided the project into two tracks:

1. Consistent Labeling and Display of Whois for all gTLDs
   - Draft Policy republished for public comment 21 October 2016
   - Target effective date – 1 August 2017

2. Transition of .COM, .NET and .JOBS from Thin to Thick Whois
   - Draft Policy published for public comment 26 October 2016
   - Target effective date for new registrations – 1 May 2018
   - Target effective date for existing registrations – 1 February 2019

Replacing the WHOIS Protocol – Background

SSAC's SAC 051 (September 2011): "The ICANN community should evaluate and adopt a replacement domain name Registration Data Access Protocol (RDAP)". The current Whois protocol:

- Only provides rudimentary functionality
- Is heavily constrained by the lack of a data model
- Lacks standardized output, internationalization, and more

IETF published the RDAP RFCs (March 2015); benefits include

- Standardization – Easier to use
- Uniformity – Easier to understand
- Supporting internationalized domain names & registration data
- Secure access to data

All but 7 gTLD registry contracts contain provisions regarding RDAP, as well as the 2013 Registrar Accreditation Agreement

Registration Data Access Protocol – Current Status

Version 1.0 of RDAP Profile mapping RDAP features to allowable policy and contractual requirements published (July 2016)

Implementation of the RDAP Profile was initially required in the Consistent Labeling & Display Policy

- RySG submitted a "Request for Reconsideration" regarding the inclusion of the RDAP Profile in the Consistent Labeling & Display policy, among other things

ICANN plans to request RDAP implementation, via existing contractual requirements, once the Consistent Labeling & Display policy is finalized and following consultations with the community

Translation and Transliteration of Contact Information

Background:

Policy Recommendations approved by Board in (September 2015)

- Registries and registrars may voluntarily translate and/or transliterate registration data
- Policy recommendations provide some requirements for how registries and registrars may translate and transliterate registration data
- Policy recommendations also require working to coordinate implementation with other WHOIS efforts

Current Implementation Status:

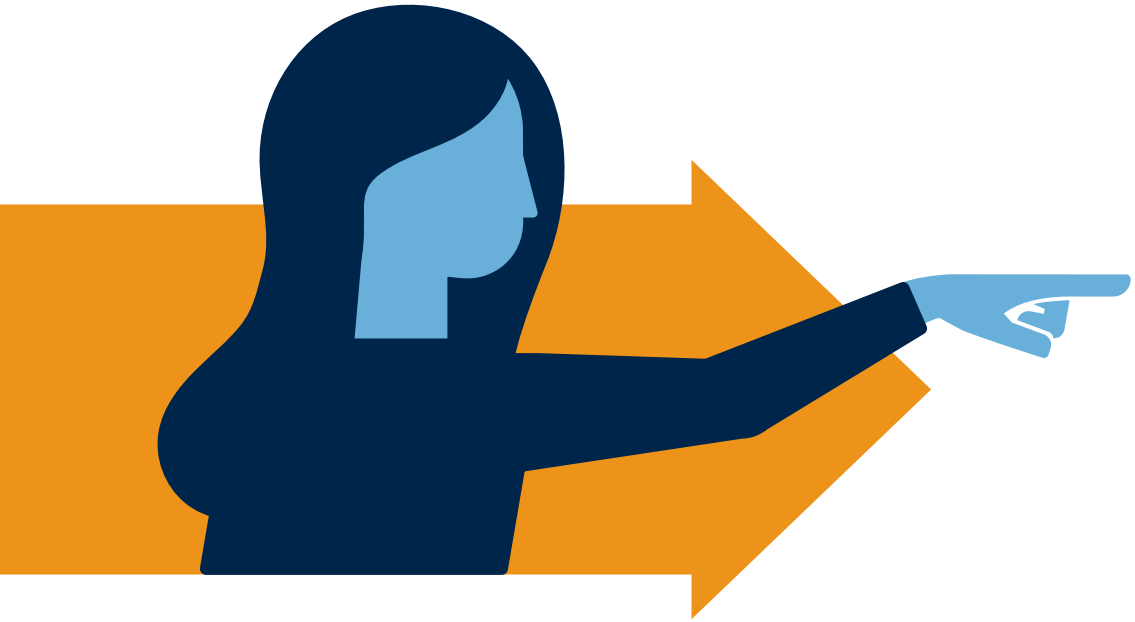
- GDD Staff and Implementation Review Team are in early stages of discussing requirements for the scope of the policy implementation project
- GDD Staff and IRT examining early drafts of policy language

The future of Whois/RDS: RDS Review Team

Margie Milam
Vice President, Multi-Stakeholder Strategic Initiatives, ICANN


Call for Volunteers!
ICANN
Registration Directory Services (RDS) Review
(formerly known as WHOIS2)

The Global Community Needs You



Help keep RDS/WHOIS

Accurate, Accessible, and Safe.

Be a part of the ICANN Review Team that will analyze and make recommendations on the requirements for consistency, efficiency, and effectiveness of registration directory services!

SO/AC Leader Limited Scope Proposal

- **Continued Community Bandwidth Concerns** in light of all of the many WHOIS related activities underway
- **Collaboration with the Board Working Group on RDS** to conduct Review more effectively, to minimize the impact to all
- **Proposal for Limited Scope Review** under consideration by the SO/AC Leadership

Limited Scope Proposal

"Post Mortem" on implementation from 1st WHOIS RT

- Small group of RT members who participated in or tracked closely the 1st WHOIS Review Team
- ICANN org "self-assessment" on:
  - Whether each rec was followed/implemented;
  - Effectiveness in addressing issues identified
  - Need for additional implementation
- **Exclude:** Issues covered by the PDP on Next Gen RDS
- **Focus:** RT evaluates self-assessment and augments it to create a full evaluation of 1st WHOIS RT recs.

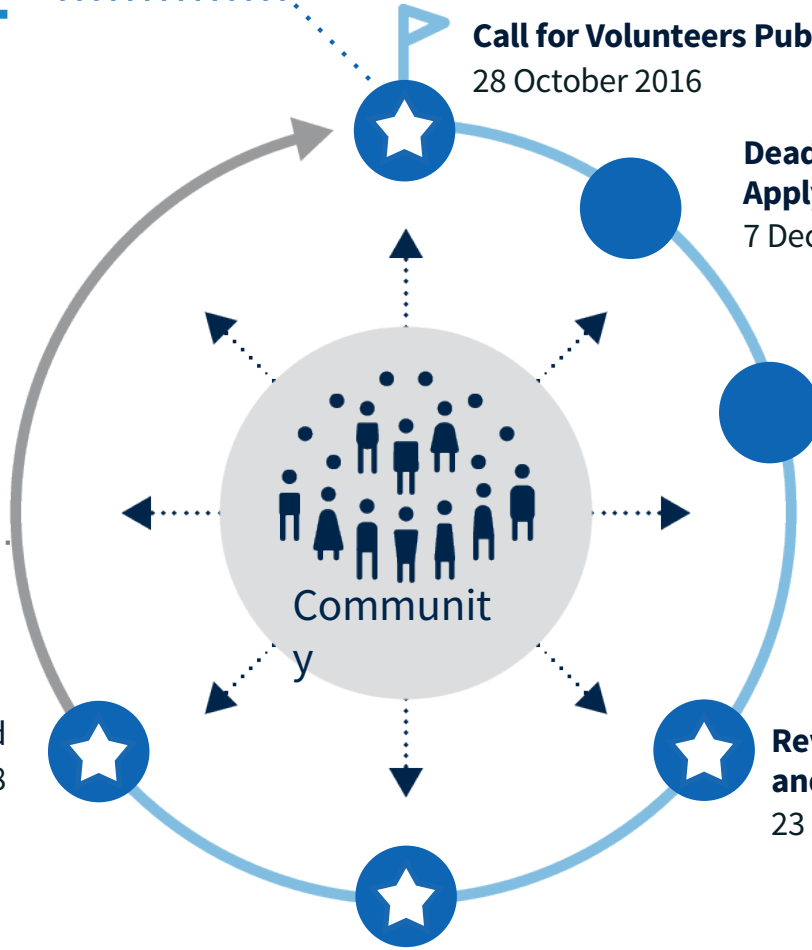
Work to be done within six months

RDS/WHOIS Review Dates and Deadlines

TARGETED TIMELINE

= Key Deadlines

RECOMMENDATION IMPLEMENTATION PROCESS



Call for Volunteers Published
28 October 2016

Deadline to Apply for Review Team
7 December 2016

Publication of Applicants
10 January 2017

Review Team Selected and Announced
23 February 2017

1st Review Team Meeting
11-16 March 2017

Estimate Final Report Published
10-15 March 2018

Note that this timeline may shorten to six months if the scope of the RDS review is limited

Thanks for Your Interest!

Please consider applying for the RDS/WHOIS Review.

Find additional details, the application, and the selection process details at

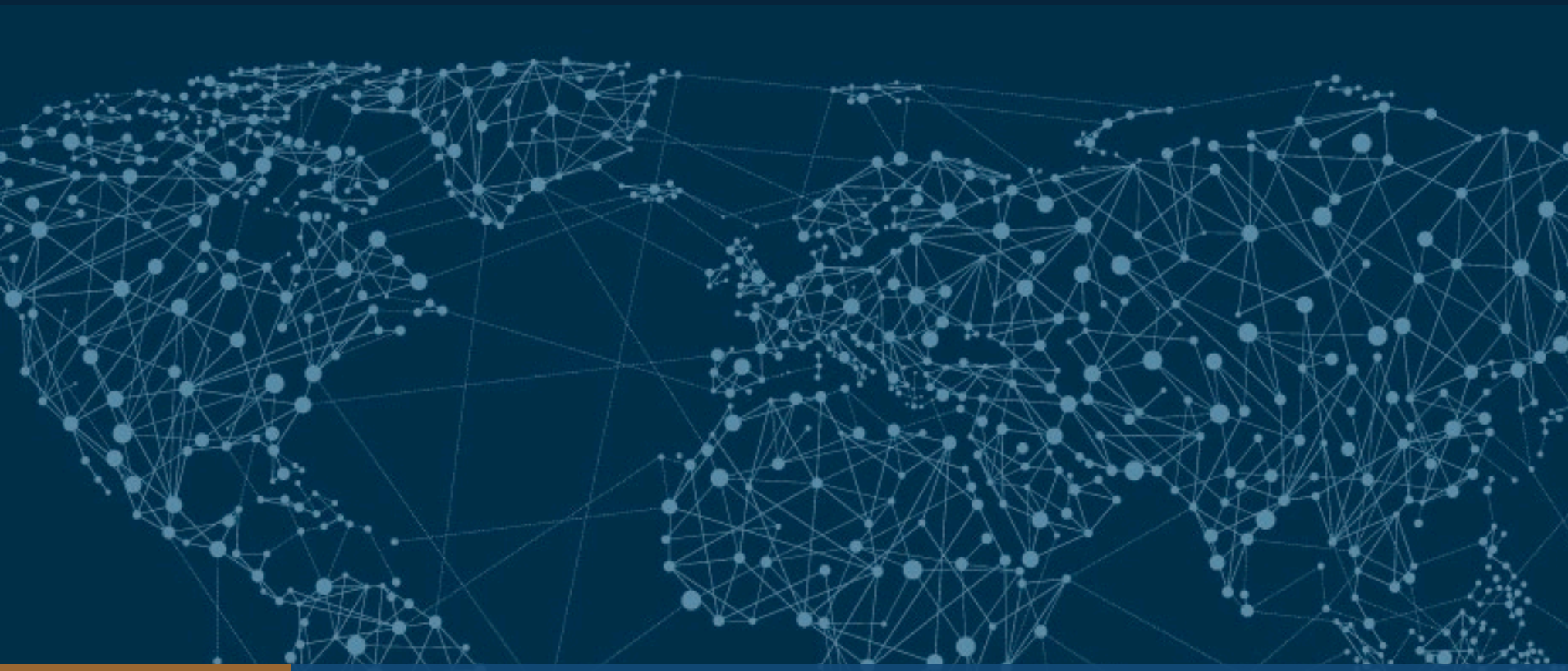
https://www.icann.org/news/announcement-2-2016-10-28-en

We look forward to receiving your application!

The future of Whois/RDS: Registration Directory Services PDP

Chuck Gomes
Chair RDS PDP WG

ICANN

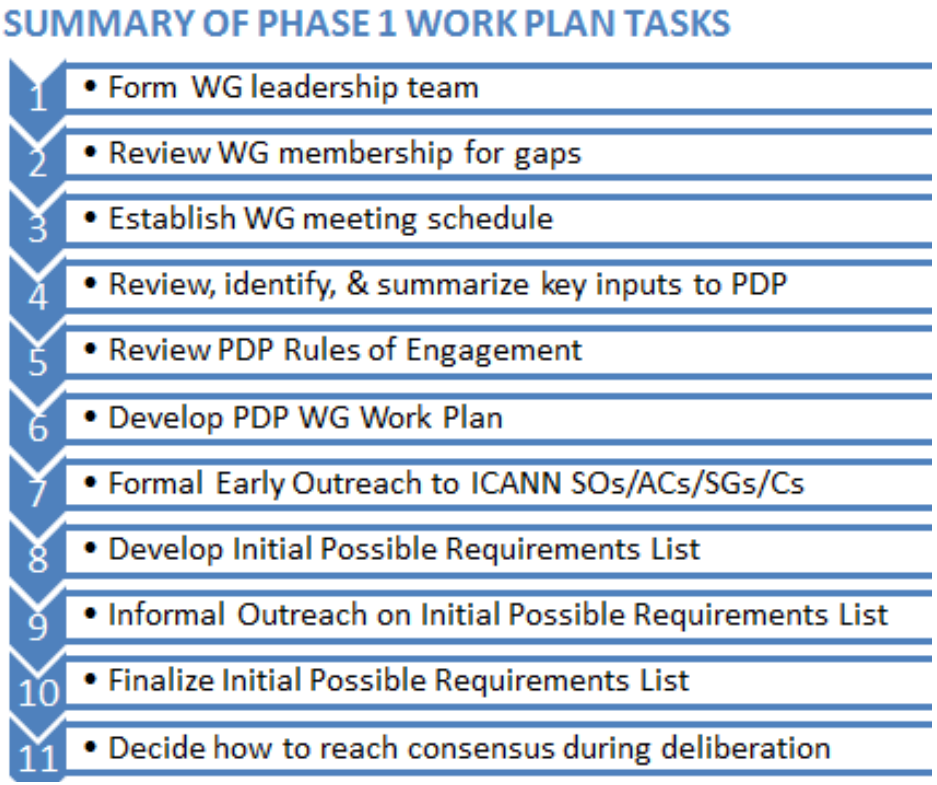


Next-Generation Registration Directory Services to Replace WHOIS PDP

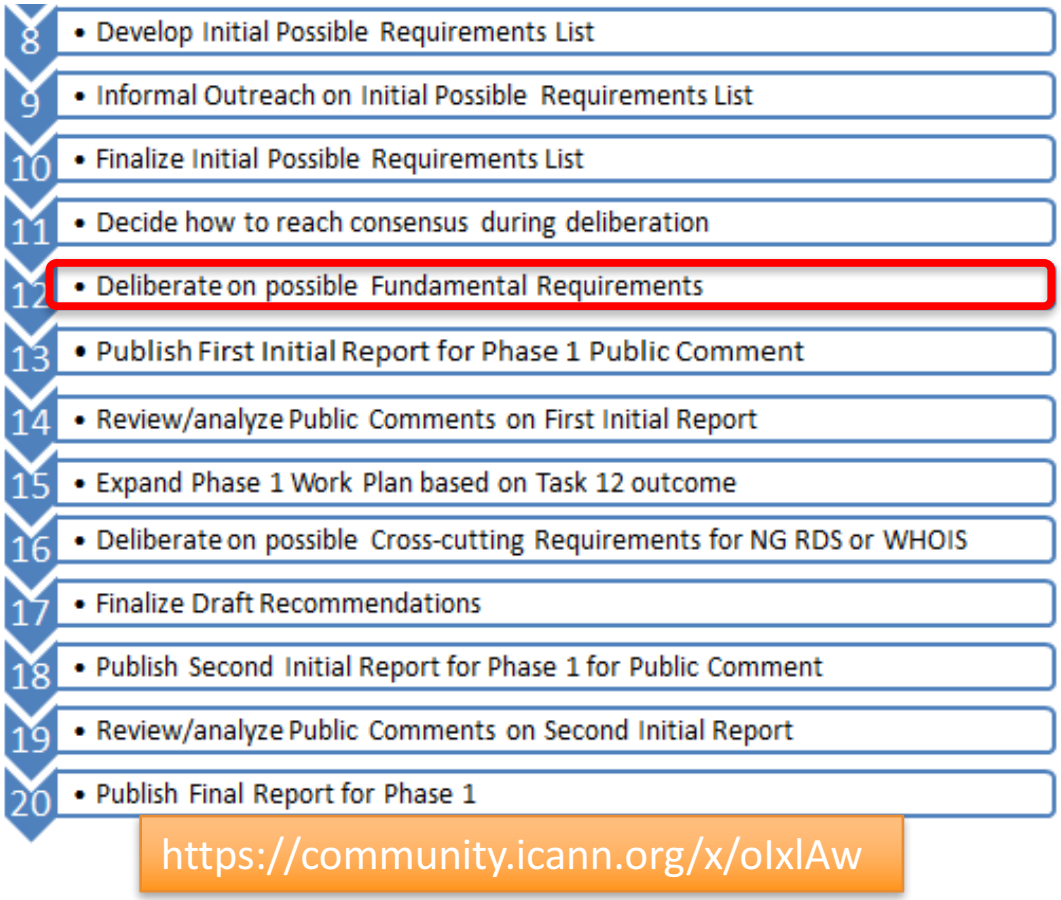
Chuck Gomes, Chair
Friday 4 November

What have we accomplished so far?

- **Approved Work Plan**, including
  - Approach to reach Consensus
- Key Input Summaries for
  - Users & Purposes
  - Data Elements
  - Privacy
- **Initial Possible Requirements List** (in progress), incorporating
  - Extracts from Key Inputs
  - Early Outreach responses
  - PDP Phase(s)
  - Dependencies
  - Codes and Keywords
- Further materials to prepare for deliberations
  - **Problem statement for this PDP WG**
  - **Representative set of example use cases**
  - **Registration data and directory service statement of purpose**



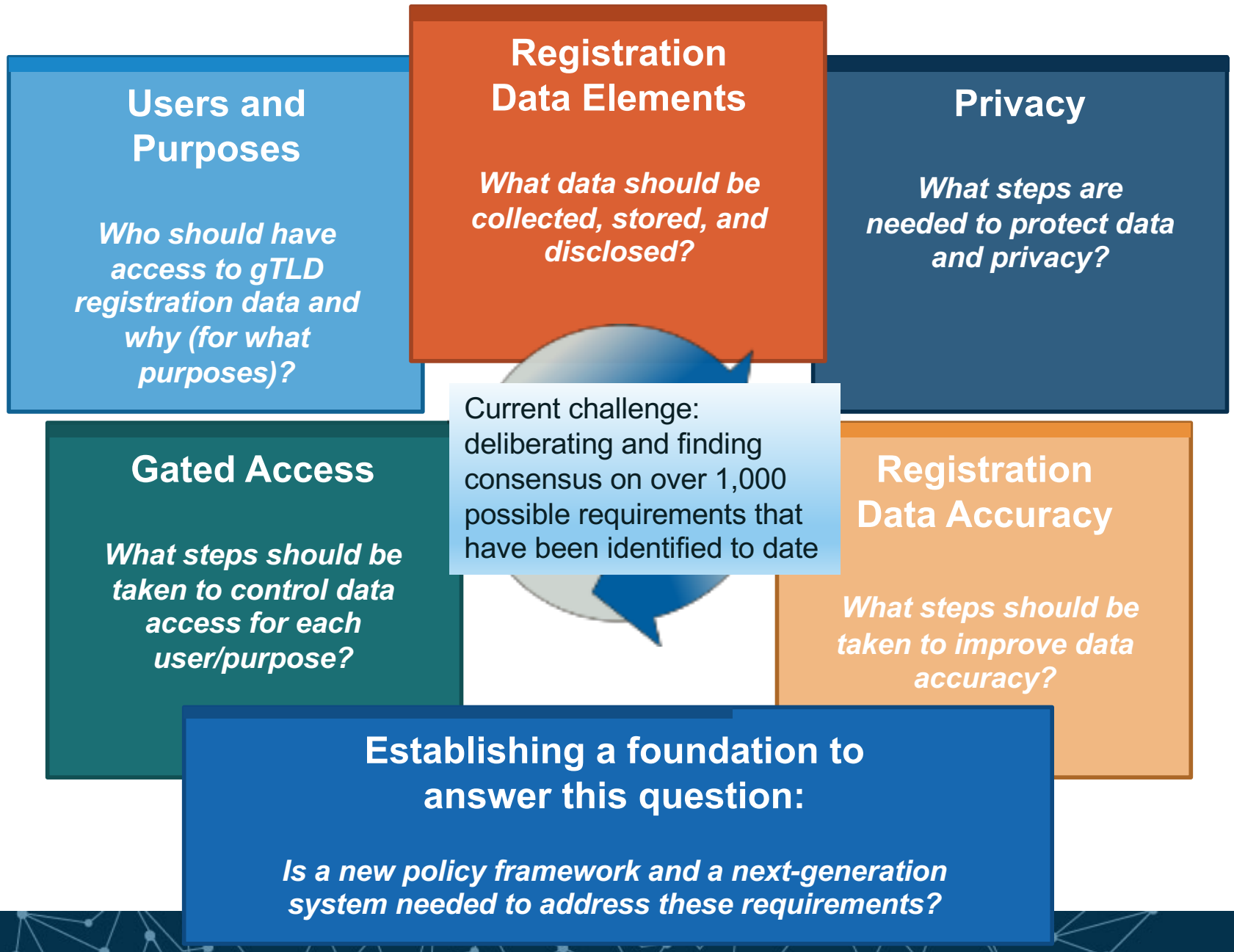
It's now time to start deliberations



Task 12.a: Deliberate on Possible Fundamental Requirements,
starting with a first pass at deliberating on requirements for these three charter questions:

- Users/Purposes: Who should have access to gTLD registration data and why?
- Data Elements: What data should be collected, stored, and disclosed?
- Privacy: What steps are needed to protect data and privacy?

Current challenges & issues under discussion



How can the GNSO Council & ICANN community assist?

- Participate and/or follow the deliberations, either as a member or as an observer
- Check progress and information available on the WG wiki (https://community.icann.org/x/rjJ-Ag)
- Provide input in response to formal and informal requests for input
- Be ready and willing to compromise – finding consensus will depend on the willingness of all involved
- Continue to ensure that all impacted SGs and Cs and ACs are actively participating in the WG.

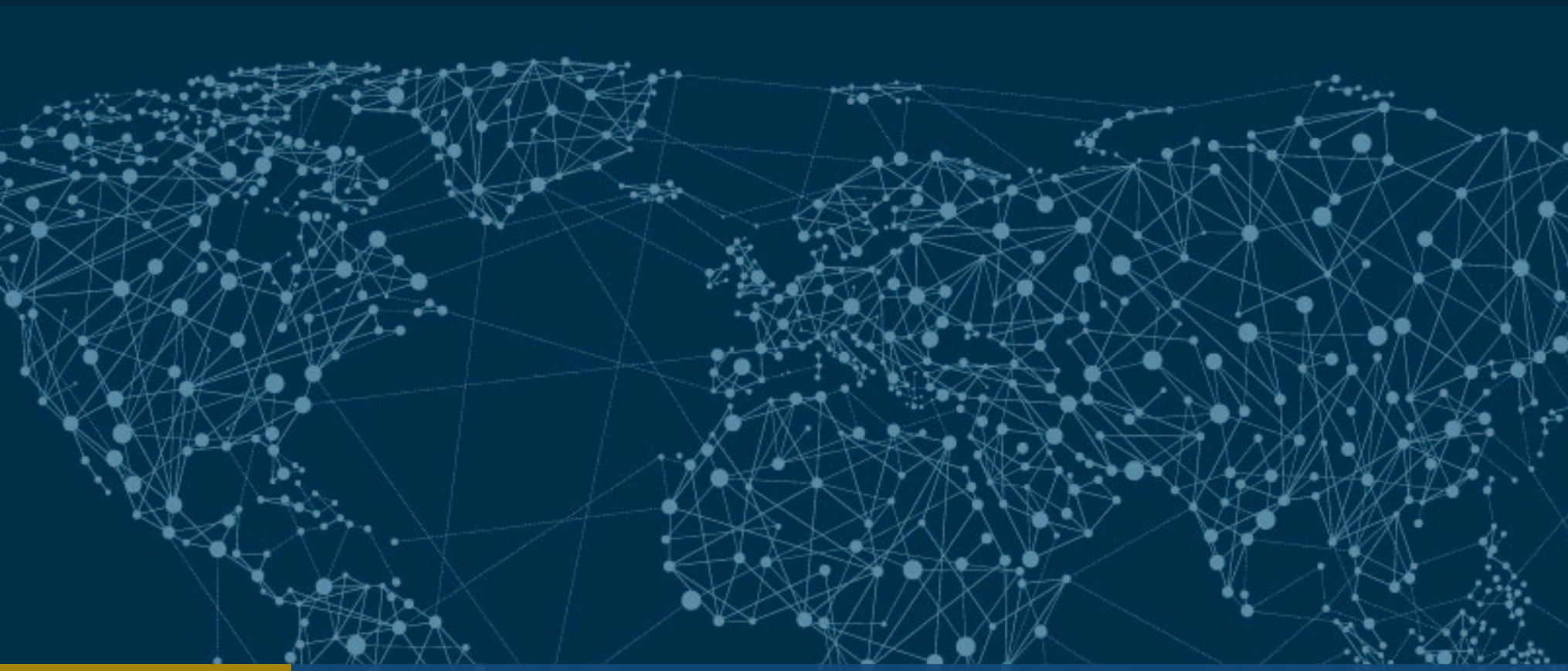
Sessions at ICANN57 and Further Information

- PDP WG F2F Meeting – Thursday 3 November (http://sched.co/8cxj)
- Update on WHOIS related initiatives – Saturday 5 November (http://sched.co/8cyZ)
- PDP WG Charter: https://community.icann.org/x/E4xlAw
  - Charter Questions and Key Inputs for each Question
  - RDS-PDP-Phase1-FundamentalQs-SubQs-MindMap
- PDP WG Work Plan: https://community.icann.org/x/oIxlAw
  - Approach to consensus in deliberation of possible requirements
- Phase 1 Outputs: https://community.icann.org/x/p4xlAw, including
  - Draft 4: RDS PDP Initial List of Possible Requirements for gTLD registration data and directory services (Draft 5 underway)
  - Draft Registration Data and Directory Service Statement of Purpose (work in progress)

The future of Whois/RDS: Privacy & Proxy Services Accreditation

Graeme Bunton
co-Chair PPSAI PDP WG

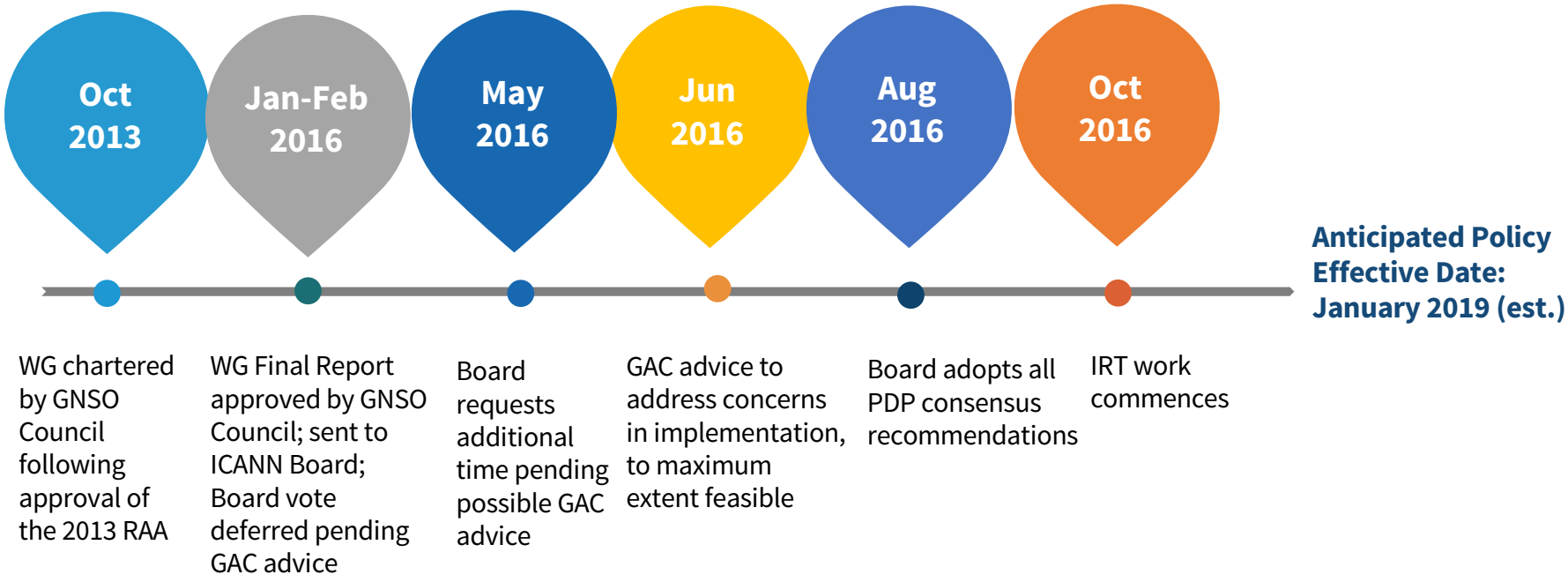
ICANN



Privacy & Proxy Services Accreditation Issues (PPSAI) Policy Development Process

Graeme Bunton (PDP Working Group Co-Chair)

OVERVIEW: PDP Timeline & Major Milestones



SCOPE OF THE PDP

This PDP was launched by the GNSO Council, at the Board's request, to develop policy principles that will guide ICANN"s implementation of an Accreditation Program for providers of Privacy & Proxy Services to domain name registrants/customers

Final PDP Recommendations: Summary

1. **Definitions**
2. **Mandatory Provisions for Customer Agreements**
3. **Best Practices & Principles for De-Accreditation**
4. **Contactability / Responsiveness of Providers**
5. **Relay, Abuse Report Requirements**
6. **Illustrative IP Disclosure Framework**

Recommendations relating to Law Enforcement (1/3)

- **Illustrative Disclosure Framework developed to apply to intellectual property owners' requests for disclosure of P/P customer information; but Working Group did not feel able to develop a similar framework for law enforcement, anti-abuse or consumer authority requests**
  - Scope of the Illustrative IP Disclosure Framework:
    - *Certain information must be provided when requesting disclosure; non-exhaustive grounds for refusal of a request; possibility of neutral dispute resolution/appeal; periodic review recommended*
  - How a Law Enforcement Framework might be different:
    - *Certain concerns may mandate a different scope or provision, e.g. need to preserve confidentiality of an investigation*
    - *Based on community feedback, WG recommends that accredited P/P service providers comply with express requests from LEA not to notify a customer where this is required by applicable law. This should not prevent providers from either voluntarily adopting more stringent standards or from cooperating with LEA*

Recommendations relating to Law Enforcement (2/3)

- **Minimum mandatory requirements to be included if a Disclosure Framework is developed for LEA requests:**
  - (a) requester agrees to comply with all applicable data protection laws and to use any information disclosed to it solely for the purpose to determine whether further action on the issue is warranted, to contact the customer, or in a legal proceeding concerning the issue for which the request was made; and
  - (b) disclosure exempted where the customer has provided, or the P/P service provider has found, specific information, facts, and/or circumstances showing that disclosure will endanger the safety of the customer

- **GAC Communique, ICANN56 (June 2016):**
  - *"GAC input and feedback should be sought out as necessary in developing a proposed implementation plan, including through participation of the Public Safety Working Group on the Implementation Review Team."*

- **GAC Community Discussion at ICANN56**

Recommendations relating to Law Enforcement (3/3)

- **Board resolution adopting PDP recommendations (Aug 2016):**
  - *"Will consider the GAC's advice and provide input to the Implementation Review Team for consideration in implementation planning."*
- **ICANN56 – GAC-hosted discussion with the community:**
  - A LEA Disclosure Framework could include:
    - *appropriate authorization and confidentiality requirements for law enforcement requests linked to ongoing investigations*
    - *address processes for P/P service providers to respond to requests from jurisdictions other than their own.*
    - *De-accreditation process that could provide the means to revoke the accreditation*
    - *of providers harboring actors engaged in deceptive, unfair, or fraudulent conduct or repeatedly not responding to LEA requests*
  - Participation of the PSWG/GAC and other community members in the IRT will be helpful in informing further discussions on this topic

Engage with ICANN

Thank You and Questions

Reach us at:
Email: engagement@icann.org
Website: icann.org

twitter.com/icann

soundcloud.com/icann

facebook.com/icannorg

weibo.com/ICANNorg

youtube.com/user/icannnews

flickr.com/photos/icann

linkedin.com/company/icann

slideshare.net/icannpresentations